UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/537,915	06/08/2005	Miyako Ohkubo	273567US90PCT	4748

22850 7590 04/03/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
REVAK, CHRISTOPHER A	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/03/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	**Application No.** 10/537,915	**Applicant(s)** OHKUBO ET AL.	
	Examiner Christopher A. Revak	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 June 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9-17,19-21,26,28,30,32,34,35,37-40,42-52,64 and 68* is/are allowed.

6)□ Claim(s) *1,18,22-25,27,29,31,33,36,41,53-63,65-67 and 69* is/are rejected.

7)□ Claim(s) *2-8* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 June 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *7/1/05; 9/2/08*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted are is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally **limited to a single paragraph** on a separate sheet within the range of 50 to 150 words. It is important that **the abstract not exceed 150 words in length** since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

5. In the instant application, the abstract exceeds the 150 word limit and is written in two paragraphs.

6. The disclosure is objected to because of the following informalities:

On page 2, line 19, reference is made to “non-patent literature 2” which is unclear which docket the application discusses in this portion of the specification. The name of the document should be listed in the specification.

On page 3 of the specification, paragraph 5, reference is made to patent applications which have the attorney docket numbers and lack the U.S. serial application numbers. The same information is similarly recited on page 4, paragraph 7.

Appropriate correction is required.

7. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code on page 2, line 16. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 55-62 and 66 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claims 55 and 58, it is recited “generating a second privileged ID, the association of which with the first privileged ID is difficult to follow”. According to previous claims, the difficulty of following the association is either tied to an inverse function or by encryption. These claims fail to particularly describe "how it is difficult to follow".

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1,18,22-25,27,29,31,33,36,41,53,54,58-63,65-67, and 69 are rejected under 35 U.S.C. 102(e) as being anticipated by Howard et al, U.S. Patent 6,629,198.

As per claim 1, it is taught of a tag privacy protection method for preventing privacy information of a user from being acquired from information which is delivered from a tag device, in which a confidential value corresponding to each tag ID information is stored in a confidential value memory of each tag device; comprising the steps of the tag device delivering tag output information which corresponds to a confidential value in the confidential value memory from an output section; and reading out at least part of elements of the confidential value from the confidential value memory, applying thereto a first function, an inverse image of which is difficult to obtain, and updating the confidential value in the confidential value memory with a result of such calculation by overwriting in a first calculator (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 18, it is disclosed of a backend apparatus for use in an automatic tag identification system comprising a database memory in which each tag ID information and a corresponding confidential value are related to each other; an input section which accepts tag output information as an input; a calculator for applying a first function F1 which is used in a tag device some number of times to at least part of elements of the confidential value in the database memory and which then applies a second function which is used in the tag device thereto; a comparator for sequentially comparing a result of the calculation in the calculator against the tag output information; and a reader for extracting the tag ID information which is related to the confidential value corresponding to the matching result of calculation when a matching between the result of calculation and the tag output information is found from the database memory (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 22, it is taught of a backend apparatus for use in an automatic tag identification system comprising a database memory in which each tag ID information id.sub.n (n.epsilon.{1, . . . , m}, where m represents a total number of tag devices) and a second confidential value s.sub.n, 1 corresponding thereto are related to each other; an input section which accepts tag output information F2(s.sub.k, i) as an input; a third calculator connected to the database memory for reading out the second confidential value s.sub.n, 1 from the database memory, applying j times (j.epsilon.{0, . . . , j.sub.max}) a first function F1 which is used in a tag device to each of the second confidential values s.sub.n, 1 which are read out, and for subsequently applying a second function F2 which is used in the tag device; a comparator for comparing the tag output information F2(s.sub.k, i) against a result of calculation in the third calculator F2(F1.sup.j(s.sub.n, 1)); a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least one of n and j in the event the tag output information F2(s.sub.k, i) and the result of calculation F2(F1.sup.j(s.sub.n, 1)) do not match; and a reader connected to the database memory and operative when the tag output information F2(s.sub.k, i) matches the result of the calculation F2(F1.sup.j(s.sub.n, 1)) to extract the tag ID information id.sub.n which is related to the second confidential value s.sub.n, 1 corresponding to the matching result of the calculation F2(F1.sup.j(s.sub.n, 1)) from the database memory (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 23, it is disclosed wherein the input section accepts an input of information which specifies a number of times m the first confidential value is updated in the tag device, the third calculator applies the first function F1 j=rn times to each of the confidential values s.sub.n, 1 which are read out and then applies the second function F2 thereto, and the controller causes the processings in the third calculator and the comparator to be executed again by changing the value of n when the tag output information F2(s.sub.k, j) does not match the result of the calculation F2(F1.sup.j(s.sub.n, 1)) (col. 9, lines 6-35).

As per claim 24, it is taught wherein the database memory stores the result of the calculation F2(F1.sup.j(s.sub.n, 1)) in the third calculator in a manner relating it to the second confidential value s.sub.n, 1, and the comparator performs a comparing processing by using the result of the calculation F2(F1.sup.j(s.sub.n, 1)) stored in the database memory (col. 9, lines 6-35).

As per claim 25, it is disclosed of a backend apparatus for use in an automatic tag identification system comprising a database memory in which each tag ID information id.sub.n (n.epsilon.{1, . . . , m}), a corresponding second confidential value s.sub.n, 1 and second proper value w.sub.n are stored in a manner relating to each other; a input section which accepts an input of tag output information F2(s.sub.k, i); a third calculator connected to the database memory for reading out the second confidential value s.sub.n, 1 and the second proper value w.sub.n from the database memory and for applying a second function F2 to I.sup.j(n) where I.sup.j(n)=s.sub.n, 1(j=0), and I.sup.j(n)=F1(I.sup.j-1(n)|id.sub.n) (j.gtoreq.1) to calculate F2(I.sup.j(n)); a comparator for comparing the tag output information F2(s.sub.k, i) against the result of the calculation in the third calculator F2(I.sup.j(n)); a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least one of n and j when the tag output information F2(s.sub.k, i) does not match the result of the calculation F2(I.sup.j(n)); and a reader for extracting tag ID information id.sub.n which is related to the second confidential value s.sub.n, 1 and the second proper value w.sub.n corresponding to the matched result of calculation F2(I.sup.j(n)) from the database memory when a matching between the tag output information F2(s.sub.k, i) and the result of the calculation F2(I.sup.j(n)) is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 27, it is taught of a backend apparatus for use in an automatic tag identification system comprising a database memory in which each tag ID information id.sub.n (n.epsilon.{1, . . . , m}) and a corresponding second confidential value s.sub.n, 1 and second proper value w.sub.n are stored in a manner relating to each other; an input section which accepts an input of tag output information F2(s.sub.k, i|w.sub.k); a third calculator connected to the database memory for reading out the second confidential value s.sub.n, 1 and the second proper value w.sub.n from the database memory, applying j times (j.epsilon.{0, . . . , j.sub.max}) a first function F1 which is used in a tag device to the second confidential value s.sub.n, 1, determining a bit combination value F1.sup.j(s.sub.n, i)|w.sub.n of a result of application F1.sup.j(s.sub.n, i) and the second proper value w.sub.n, and applying a second function F2 which is used in the tag device to the bit combination value F1(s.sub.n, i|w.sub.n); a comparator for comparing the tag output information F2(s.sub.k, i|w.sub.k) against a result of calculation in the third calculator F2(F1.sup.j(s.sub.n, i)|w.sub.n); a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least one of n and j when the tag output information F2(s.sub.k, i|w.sub.k) does not match the result of the calculation F2(F1.sup.j(s.sub.n, i)|w.sub.n); and a reader connected to the database memory for extracting the tag ID information id.sub.n which is related to the second confidential value s.sub.n, 1 and the second proper value w.sub.n corresponding to the matched result of calculation F2(F1.sup.j(s.sub.n, i)|w.sub.n) when a matching between the tag output information

F2(s.sub.k, i|w.sub.k) and the result of the calculation F2(F1.sup.j(s.sub.n, i)|w.sub.n) is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 29, it is disclosed of a backend apparatus for use in an automatic tag identification system comprising a database memory in which each tag ID information id.sub.n (n.epsilon.{1, . . . , m}) and a corresponding second proper value w.sub.n are stored in a manner relating to each other; a calculated value memory in which first results of calculation s.sub.j+1 are stored which are obtained by applying j times (j.epsilon.{0, . . . , j.sub.max}) a first function which is used in a tag device to a second confidential value s.sub.1 which is used in common for a plurality of tag ID information; an input section which accepts an input of tag output information F2(s.sub.i|w.sub.k); a third calculator connected to the database memory for reading out the first result of calculation s.sub.j+1 and the second proper value w.sub.n from the database memory to obtain a bit combination value thereof s.sub.j+1|w.sub.n and for applying a second function F2 which is used in the tag device thereto; a comparator for comparing the tag output information F2(s.sub.i|w.sub.k) and the result of calculation in the third calculator F2(s.sub.j+1|w.sub.n); a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least one of n and j when the tag output information F2(s.sub.i|w.sub.k) does not match the result of calculation F2(s.sub.j+1|w.sub.n); and a reader connected to the database memory for extracting the tag ID information id.sub.n which is related to the second proper value w.sub.n corresponding to the matched result of calculation F2(s.sub.j+1|w.sub.n) when a matching between the tag output information

F2(s.sub.i|w.sub.k) and the result of calculation F2(s.sub.j+1|w.sub.n) is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 31, it is taught of a backend apparatus for use in an automatic tag identification system comprising a database memory in which a combination of d initial elements f.sub.u, 0 comprising one selected from each of d kinds (d.gtoreq.2) of subgroups .alpha..sub.u(u.epsilon.{1, . . . , d}), and tag ID information id.sub.n of each tag device n (n.epsilon.{1, . . . , m}, where m represents a total number of tag devices) are stored in a manner relating to each other; an input section for accepting an input of tag output information a.sub.k, i; a third calculator for applying w.sub.u times (w.sub.u.epsilon.{1, 2, . . . , max}) a first function F1 to the d initial elements f.sub.u, 0 (u.epsilon.{1, . . . , d}) which correspond to the tag ID information id.sub.n and for applying a second function F2 to a bit combination value of these values F1.sup.wu(f.sub.u, 0) to determine a calculated value c; a comparator for comparing the tag output information a.sub.k, i against the calculated value c; a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least part of n and w.sub.u when the tag output information a.sub.k, i does not match the calculated value c; and a reader connected to the database memory for extracting tag ID information id.sub.n which is related to the combination of d initial elements f.sub.u, 0 corresponding to the calculated value c when the tag output information a.sub.k, i matches the calculated value c (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 33, it is disclosed of a backend apparatus for use in an automatic tag identification system comprising a database memory in which a combination of d initial elements f.sub.u, 0 comprising one selected from each of d kinds (d.gtoreq.2) of subgroups .alpha..sub.u (u.epsilon.{1, . . . , d}), a proper value .gamma..sub.n which is inherent to each tag ID information id.sub.n (n.epsilon.{1, . . . , m}) and each tag ID information id.sub.n are stored in a manner relating to each other; an input section for accepting an input of tag output information a.sub.k, i; a third calculator for applying w.sub.u times (w.sub.u.epsilon.{1, 2, . . . , max}) a first function F1 to the d initial elements f.sub.u, 0 (u.epsilon.{1, . . . , d}) corresponding to the tag ID information id.sub.n and for applying a second function F2 to a bit combination value of these values F1.sup.wu(f.sub.u, 0) and the proper value .gamma..sub.n to determine a calculated value c; a comparator for comparing the tag output information a.sub.k, i against the calculated value c; a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value of at least part of n and w.sub.u when the tag output information a.sub.k, i does not match the calculated value c; and a reader connected to the database memory for extracting tag ID information id.sub.n which is related to the combination of a plurality of initial elements f.sub.u, 0 corresponding to the calculated value c from the database memory when a matching between the tag output information a.sub.k, i and the calculated value c is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 36, it is taught of a backend apparatus for use in an automatic tag identification system comprising a database memory in which a combination of d initial elements f.sub.u, 0 comprising one selected from each of d kinds (d.gtoreq.1) of subgroup .alpha..sub.u (u.epsilon.{1, . . . , d}) and a tag ID information id.sub.n (n.epsilon.{1, . . . , m}) of each tag device are stored in a manner relating to each other; a second manifold value memory in which a manifold value z which assumes t kinds (t.gtoreq.2) of values is stored; an input section for accepting an input of tag output information a.sub.k, i; a third calculator for applying w.sub.u times (w.sub.u.epsilon.{1, 2, . . . , max}) a first function F1 to the d initial elements f.sub.u, 0 (u.epsilon.{1, . . . , d}) in the database memory which correspond to the tag ID information id.sub.n and for applying a second function F2 to a bit combination value of these values F1.sup.wu(f.sub.u, 0) and the manifold value z in the second manifold value memory to determine a calculated value c; a comparator for comparing the tag output information a.sub.k, i against the calculated value c; a controller for causing the processings in the third calculator and the comparator to be executed again by changing the value at least part of n, w.sub.u and z when the tag output information a.sub.k, i does not match the calculated value c; and a reader connected to the database memory for extracting the tag ID information id.sub.n which is related to the combination of d initial elements f.sub.u, 0 corresponding to the calculated value c from the database memory when a matching between the tag output information a.sub.k, i and the calculated value c is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 41, it is disclosed of a backend apparatus for use in an automatic tag identification system comprising a database memory in which a combination of d initial elements f.sub.u, 0 which comprises one selected from each of d kinds (d.gtoreq.1) of subgroups .alpha..sub.u (u.epsilon.{1, . . . , d}) and tag ID information id.sub.n (n.epsilon.{1, . . . , m}) of each tag device are stored in a manner relating to each other; a second manifold value memory in which a manifold value z.sub.u which assumes t.sub.u kinds (t.sub.u.gtoreq.2) of values for each u is stored; an input section for accepting an input of tag output information a.sub.k, i; a third calculator for applying w.sub.u times (w.sub.u.epsilon.{1, 2, . . . , max}) a first function F1 which is used in a tag device to the d initial elements f.sub.u, 0 (u.epsilon.{1, . . . , d}) corresponding to the tag ID information id.sub.n and for applying a second function F2 which is used in the tag device to a bit combination value of these values F1.sup.wu(f.sub.u, 0) and the manifold value z.sub.u to determine a calculated value c; a comparator for comparing the tag output information a.sub.k, i against the calculated value c; a controller for causing the processing in the third calculator and the comparator to be executed again by changing the value of at least part of n, w.sub.u and z; and a reader connected to the database memory for extracting tag ID information id.sub.n which is related to the combination of the d initial elements f.sub.u, 0 corresponding to the calculated value c from the database memory when a matching between the tag output information a.sub.k, i and the calculated value c is found (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 53, it is taught of an update solicitor for soliciting an updater to update privileged ID information in a tag device, the update solicitor being provided externally of the tag device and comprising a privileged ID input section to which a plurality of kinds of privileged ID's, which are re-encryptable encrypted texts corresponding to an identical tag ID information id.sub.h, are input; a privileged ID memory for storing a plurality of kinds of privileged ID's which are input thereto; a privileged ID extractor connected to the privileged ID memory for extracting one of privileged ID's from the privileged ID memory at a given opportunity; and a privileged ID output section for delivering the extracted privileged ID to the tag device (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 54, it is disclosed of a tag device for use in an automatic tag identification system comprising a privileged ID input section to which a plurality of kinds of privileged ID's, which are re-encryptable encrypted texts corresponding to an identical tag ID information id.sub.h, are input; a privileged ID memory for storing the plurality of kinds of privileged ID's which are input thereto; a privileged ID extractor connected to the privileged ID memory for extracting one of the privileged ID's from the privileged ID memory at a given opportunity; and a privileged ID output section for delivering the extracted privileged ID (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 58, it is taught of a tag device for use in an automatic tag identification system comprising a privileged ID memory including a read-only region in which a key ID is stored and a rewritable region in which a first privileged ID is stored; a read/write section for extracting the key ID and the first privileged ID from the privileged ID memory; a first output section for delivering the key ID and the first privileged ID which are extracted; and a second input section for accepting an input of a second privileged ID, the association of which with the first privileged ID is difficult to follow; the read/write section storing the second privileged ID which is input in the rewritable region of the privileged ID memory (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 59, it is disclosed of a tag device in which the second input section additionally accepts an input of verification information for the second privileged ID and the read/write section additionally stores the verification information which is input in the rewritable region of the privileged ID memory (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 60, it is taught of a tag device in which the privileged ID represent information which is part of information constituting an ID and which is inherent to each tag device, which is privileged alone (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 61, it is disclosed of a tag device in which an identical key ID is allocated to unrelated tag devices (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 62, it is taught of a tag program for enabling a computer to function as a tag device according to one of claims 54 and 58 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 63, it is disclosed of a tag program for enabling a computer to function as a backend apparatus according to claim 18 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 65, it is taught of an update soliciting program for enabling a computer to function as an update solicitor according to claim 53 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 66, it is disclosed of a computer readable record medium storing a tag program which enables a computer to function as a tag device according to one of claims 54 and 58 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 67, it is taught of a computer readable record medium storing a tag program which enables a computer to function as a backend apparatus according to claim 18 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

As per claim 69, it is disclosed of a computer readable record medium storing an update soliciting program which enables a computer to function as an update solicitor according to claim 53 (col. 1, lines 31-48; col. 4, lines 10-17; and col. 9, lines 6-35).

Allowable Subject Matter

12. Claims 9-17,19-21,26,28,30,24,35,37-40,42-52,64, and 68 and are allowed.

13. The following is a statement of reasons for the indication of allowable subject matter:

As per claims 9-17,19-21,26,28,30,24,35, and 37-40, it was not found to be taught in the prior art of a confidential value memory in which a confidential value corresponding to tag ID information is stored. A second calculator connected to the confidential value memory for reading out the confidential value from the confidential value memory and for applying a second function F2 which disturbs a relationship between elements of a definition domain and a mapping thereof to the confidential value which is read out to generate tag output information. An output section for delivering the tag output information and a first calculator for reading out at least part of elements of the confidential value from the confidential value memory and for applying a first function F1, a mapping of which is difficult to obtain, to the elements which are read out, with a result of such calculation being used to update the confidential value in the confidential value memory by overwriting.

As per claims 42-47, it was not found to be taught in the prior art of a tag device reading out the privileged ID information sid.sub.h stored in the confidential value memory in a read/write section; and delivering the privileged ID information sid.sub.h to an updater which is provided externally of each tag device from a first output section; the updater accepting an input of the privileged ID information sid.sub.h at a first input section; generating new privileged ID information sid.sub.h', the association of which with the privileged ID information sid.sub.h is difficult to follow in an updating section; delivering the new privileged ID information sid.sub.h' to the tag device from a second output section; the tag device further accepting an input of the new privileged ID information sid.sub.h' at a second input section; the read/write section of the tag device storing the new privileged ID information sid.sub.h' in the confidential value memory.

As per claim 48, it was not found to be taught in the prior art of a privileged ID memory for storing each tag ID information id.sub.h and privileged ID information sid.sub.h which is a random value r.sub.h which corresponds to the tag ID information id.sub.h in a manner relating to each other; a first input section which accepts an input of the privileged ID information sid.sub.h which is delivered from the tag device; a random value generator for generating a new random value r.sub.h'; a second read/write section connected to the privileged ID memory for selecting tag ID information id.sub.h which corresponds to the privileged ID information sid.sub.h which is accepted by the first input section as the input from the privileged ID memory and for relating this with the new random value r.sub.h' as new privileged ID information sid.sub.h' to be stored in the privileged ID memory; and a second output section for delivering the new privileged ID information sid.sub.h' to the tag device h. Claims 49-52 recite of similar limitations.

14. Claims 2-8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Thursday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Ayaz Sheikh can be reached on 517-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2431